Quantum Key Distribution for d-level systems with Generalized Bell States

Vahid Karimipour [a] *
Saber Bagherinezhad [b] †
Alireza Bahraminasab [a‡]
[a]Department of Physics, Sharif University of Technology,
[b]Department of Computer Science, Sharif University of Technology
P. O. Box 11365-9161, Tehran, Iran

November 21, 2001

Abstract

We introduce a generalization of Hadamard and the controlled not gates which together with the generalized Bell states, enable us to introduce new methods for quantum key distribution (QKD) of d-level quantum states (qudits). In case of eavesdropping, an error rate of $\frac{d-1}{d}$ is introduced in Bob's received qudits, so that for large d, comparison of only a tiny fraction of received qudits with the sent ones detect the presence of Eve.

Keywords: d-level states, Generalized Bell States, Quantum Key Distribution.

*e-mail:vahid@sina.sharif.ac.ir.
†e-mail: bagherin@ce.sharif.ac.ir
‡e-mail: baramina@physics.sharif.edu

1 Introduction

As far as classical computation and classical communication are concerned, binary units of memory and binary logic gates play an inevitable and natural role due to the inherent simplicity of Boolean algebra on the one hand and their compatibility with states of electronic devices on the other hand. With such classical gates as NOT, AND, and OR, the simplest logical operations with which we are familiar in everyday life, can be implemented. They are also quite simple to design electronically. However in quantum computation and communication (see [1, 2] and references therein), the main resources that have the potential of surpassing our conventional classical methods, are quantum parallelism (for massive computation), non-locality and entanglement (for communication) and uncertainty relations (e.g. for Quantum Key Distribution among other things). For utilizing these resources, two level quantum states are not inevitable. Only considerations of quantum hardware should decide between using 2-level or multi level states. At present a major difficulty in quantum computation is the limit on the number of qubits that can be coupled experimentally [3]. The use of d-dimensional systems or qudits has the advantage that compared to qubits fewer systems should be coupled to obtain a given dimensionality of the Hilbert space, although it may be easier to construct universal gates for qubits than for qudits. In view of this, some aspects of quantum computation have been studied also for $d-$level systems, like consideration of quantum gates for qudits [4], quantum error correcting codes [5, 6], and generalization of the $BB84$ protocol [7] for quantum key distribution[8]. (For a review on quantum key distribution see [9].)
There has even been a lot of activity in formulating various algorithms and protocols for continuous variables (see [10, 11] and referenced therein).
In any case, we will gain more insight into the methods and algorithms of quantum computation and communication, if we study these methods for general d-level systems, in a uniform manner so that by going to specific limits we can recover the familiar results of 2-level systems or the results for continuous variables.
In this paper we are mainly concerned with a method of quantum key distribution based on d-level states, although in the way of studying this, we have derived other results about some simple algorithms, which we will present in the appendix.

The QKD scheme of BB84 [7] for qubits and its generalization to three level states or qutrits [12, 13] and to general d-level states in [8] are based on defining the key partly in the various choices of the bases chosen by Alice and Bob for encoding and decoding the different bits or dits. There are also QKD protocols for two level systems based on shared entanglement [14, 15], in which non-local properties of entanglement are exploited to secure information transfer.
Our aim in this article is to propose a quantum key distribution scheme for d-level systems, based on a protocol proposed in [15]. The key elements of our work is a generalization of the Hadamard gate and the CNOT gate for d-level systems. We will also use the generalized bell states recently introduced in [16]. We will show that by suitable manipulations of the qudits (unitary transformations), Alice and Bob can communicate securely a secret key, and can detect the presence of an eavesdropper

by comparing with each other, only a tiny fraction of their sent and received qudits. The structure of this paper is as follows. In section 2 we first review some known facts about the generalized Bell states, and then introduce the analogs of CNOT and the Hadamard gates for qudits. In section 3 we introduce the QKD scheme for d-level systems, where we also discuss one method of attack and the way around it. In section 4 which concludes the paper, we discuss a possible route to generalizing our results to the continuous variables. In the appendix we will state some further results on qudit computation and communication which are not directly related to the body of the paper, but we think are worth while of attention.

2 States, and Gates for d-level Systems

For qudits, a generalization of the familiar Bell states, has been introduced in [16]. These are a set of d^2 maximally entangled states which form an orthonormal basis for the space of two qudits. Their explicit forms are:

$$|\Psi_{m,n}\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{nj} |j, j+m\rangle \tag{1}$$

where $\zeta = e^{\frac{2\pi i}{d}}$ and m and n run from 0 to $d-1$. These states have the properties $\langle \Psi_{m,n} | \Psi_{m',n'} \rangle = \delta_{n,n'} \delta_{m,m'}$ (orthonormality) and $trace_2(|\Psi_{m,n}\rangle\langle\Psi_{m,n}|) = \frac{1}{d} I$(maximal entanglement). The following operators, first defined in [16] are also useful, since they play the analogous role of Pauli operators for qudits:

$$U_{m,n} = \sum_{j=0}^{d-1} \zeta^{nj} |j+m\rangle\langle j| \tag{2}$$

For example, given the entangled state $|\Psi_{0,0}\rangle$, only one of the parties, say Alice, can generate any Bell state $|\Psi_{m,n}\rangle$ by acting on $|\Psi_{0,0}\rangle$ with $U_{m,n}$, i.e:

$$(I \otimes U_{m,n}) |\Psi_{0,0}\rangle = |\Psi_{m,n}\rangle \tag{3}$$

One should however note that contrary to the Pauli operators, the operators $U_{m,n}$ are not necessarily Hermitian.
We now define a generalization of Hadamard gate which turns out to be quite useful in manipulating qudits for various applications.

$$H := \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \zeta^{ij} |i\rangle\langle j| \tag{4}$$

where $\zeta = e^{\frac{2\pi i}{d}}$. This operator is really not new and it is known as the quantum Fourier transform when $d = 2^n$. In that case it acts on n qubits. Here we are assuming it to be a basic gate on one single qudit, in the same way that the ordinary Hadamard gate is a basic gate on one qubit. This operator is symmetric and unitary

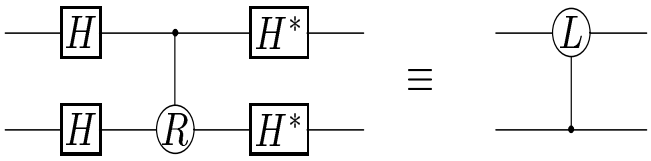

Figure 1: Circuit identity for d-level gates

$(HH^* = I)$, but not hermitian.
To generalize the NOT and the CNOT gates, we note that in the context of qudits, the NOT gate, is basically a mod-2 adder. For qudits this operator gives way to a mod-d adder, or a Right-Shift gate,

$$R|j\rangle = |j+1\rangle \qquad \text{mod} \quad d \tag{5}$$

$$R^{-1}|j\rangle \equiv L|j\rangle = |j-1\rangle \qquad \text{mod} \quad d, \tag{6}$$

where L has been used to denote a left shift. Note that $R^d = I$, compared to $NOT^2 = I$. For every unitary operator U the controlled gate U_c which acts on the second qudit conditioned on the first qudit is naturally defined as follows:

$$U_c(|i\rangle \otimes |j\rangle) = |i\rangle \otimes U^i|j\rangle \tag{7}$$

Note the difference with the qubit case. In the qubit case a controlled operator acts only if the value of the first bit is 1, here it acts i times if the value of the first qudit is i. (Sometimes it is said that a controlled operator is like an *if statement* in classical computation [1]. If we take this statement literally, then a controlled operation for d-level states acts like a loop.) In particular the controlled shift gates which play the role of CNOT gate, act as follows:

$$R_c|i,j\rangle = |i,j+i\rangle \qquad\qquad L_c|i,j\rangle = |i,j-i\rangle \tag{8}$$

Every function f from $\{0,1,\cdots,d-1\}^n \to \{0,1,\cdots,d-1\}^m$ is made reversible by the definition $f_r(\mathbf{x},\mathbf{y}) = (\mathbf{x}, f(\mathbf{x})+\mathbf{y})$ where all additions are performed mod d. In quantum circuits such a function is implemented by a unitary operator $U_f|\mathbf{x},\mathbf{y}\rangle := |\mathbf{x}, f(\mathbf{x})+\mathbf{y}\rangle$ where $\mathbf{x} \in \{0,1,\cdots,d-1\}^n$ and $\mathbf{y} \in \{0,1,\cdots,d-1\}^m$. Note that here and in all that follows addition of multi dits is performed dit-wise and mod d.
Quite analogously to the q-bits, the Hadamard and the Controlled Shift gates can generate all the Bell states $\{|\Psi_{m,n}\rangle\}$ from the computational basis states $\{|m,n\rangle\}$:

$$R_c(H \otimes I)|n,m\rangle = |\Psi_{m,n}\rangle \tag{9}$$

Many other properties of these gates are simply carried over from the case of q-bits to the general case with appropriate modifications. For example one can check the validity of the circuit identity in fig. (1).

3 Quantum Key Distribution

Quantum Key distribution with the original protocol of BB84, has already been generalized to the d-level case in [8]. Here our method of Quantum Key Distribution (QKD), is based on an idea first put forward in [15]. In this type of QKD, the two parties say Alice and Bob, use a reusable entangled state (EPR pair), to encode and decode their classical data. A third party say Eve, who tries to eavesdrop the data, will have no access to the information and moreover its presence will be detected by Alice and Bob.
The starting point of this protocol is the sharing of a Bell state $|\Psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j\rangle$ by Alice and Bob. The qudit to be sent is denoted by q. The basic idea neglecting considerations of Eve's attack for now, is that Alice performs a controlled-right shift on q and thus entangles this qudit to the the previously shared Bell state, producing the state

$$\Phi = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j,q+j\rangle_{a,b,q}. \tag{10}$$

She then sends the qudit to Bob. At the destination, Bob performs a controlled-left shift on the qudit and disentangles it from the Bell state, hence revealing the value of q with certainty.
A possible conceivable attack by Eve(e) is that she entangles her state to those of Alice(a), Bob(b) and the qudit(q) so that after Bob measurement of the qudit, she can obtain partial information about the qudit. The best way to describe and visualize the protocol is to refer to fig. (2), where the qudits are drawn as lines and states at each stage are shown explicitly.
The strategy that Eve follows should be described separately for the first qudit and the rest of the qudits. For the first qudit, she performs no measurement and proceeds so that her qudit gets entangled with the the Bell state of Alice and Bob at the end of the process. For this she uses a controlled right-shift on her qudit conditioned on the value of the first qudit being sent (see fig. (2)). The states at various stages are as follows, where in each ket the qudits refer respectively from left to right to Alice(a), Bob(b), the qudit(q) and Eve(e):

$$\Phi_0 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j,q_1,0\rangle_{a,b,q,e} \tag{11}$$

$$\Phi_1 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j,q_1+j,0\rangle_{a,b,q,e} \tag{12}$$

$$\Phi_2 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j,j,q_1+j,q_1+j\rangle_{a,b,q,e} \tag{13}$$

$$\tag{14}$$

In the last stage when Bob performs his Left-Shift he disentangles the qudit from the state of Alice, Bob and Eve. He thus reads the value of q_1, however his shared Bell

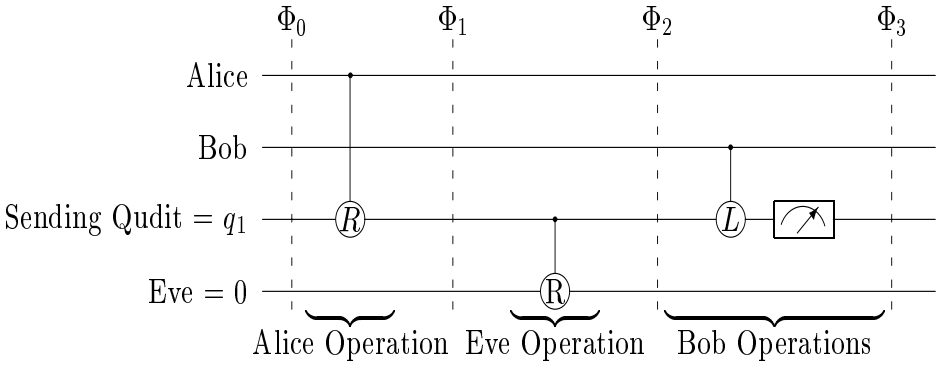

Figure 2: Eve attack for the first qudit

state with Alice has now been left entangled with the state of Eve:

$$\Phi_3 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_1 + j\rangle_{abe} \tag{15}$$

Note that this is what Eve does only for the first qudit. For the next qudits she modifies her strategy by first performing a left-shift, measuring her qudit and then performing a right-shift on her qudit. The rest of the process is like that for the first qudit (see fig. (3)). The various states in different stages shown in the figure are as follows:

$$\Phi_0 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_2, j + q_1\rangle_{a,b,q,e} \tag{16}$$

$$\Phi_1 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_2 + j, j + q_1\rangle_{a,b,q,e} \tag{17}$$

$$\Phi_2 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_2 + j, q_1 - q_2\rangle_{a,b,q,e} \tag{18}$$

$$1 \tag{19}$$

At this stage Eve measures her own qudit to be $q_1 - q_2$. The next states in the protocol are

$$\Phi_3 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_2 + j, q_1 + j\rangle_{a,b,q,e} \tag{20}$$

$$\Phi_4 = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, j + q_1\rangle_{a,b,e} |q_2\rangle_b. \tag{21}$$

$$\tag{22}$$

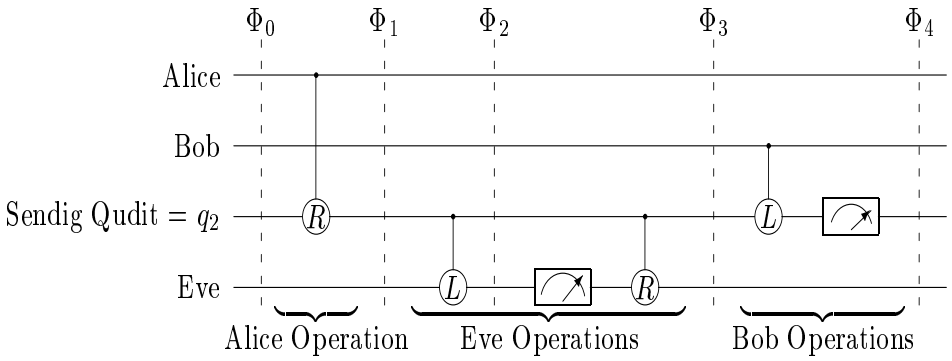

Figure 3: Eve attack for next qudits

It is now clear that Bob can measure as before the state of the qudit q_2, however Eve has also been able to obtain the value $q_1 - q_2$, while the final Bell state of Alice and Bob is again entangled with that of Eve in the form (15). This state can again be used for the other qudits of the sequence. In this way Eve intercepts the qudits $q_1 - q_2, q_1 - q_3, q_1 - q_4,$ etc, from which she can infer all the sequence by checking d possible values for q_1..

To protect this protocol against this kind of attack, Alice and Bob proceed as follows: They act on their shared Bell state by the Hadamard gates H and H^*, respectively. The key point is that a Bell state disentangled from the outside world is unchanged under this operation

$$(H \otimes H^*)|\Psi_{0,0}\rangle = |\Psi_{0,0}\rangle. \tag{23}$$

In fact the shared state is unchanged under more general operators of the form $U \otimes U^*$, where U is any unitary operator. However as we will see, the best choice of U is the Hadamard gate. It is clear from fig. (2), that for the first qudit nothing changes. However for the second qudit and other qudits, essential changes occur in the intermediate states in the process. As we will see, in this way Alice and Bob can prevent Eve from getting any useful information from entangling her state to that of Alice and Bob. The new initial state Φ_0', before Alice and Bob act on it by their Hadamard gates is

$$\Phi_0' = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j, q_2, j + q_1\rangle_{a,b,q,e} \tag{24}$$

which after action of Hadamard gates (not shown in the figure) becomes

$$\Phi_0 = \frac{1}{\sqrt{d}} \sum_{i,j,k=0}^{d-1} H_{i,j} H^*_{k,j} |i, k, q_2, j + q_1\rangle_{a,b,q,e} \tag{25}$$

The states Φ_1 and Φ_2 will be as follows:

$$\Phi_1 \quad = \quad \frac{1}{\sqrt{d}} \sum_{i,j,k=0}^{d-1} H_{i,j} H^*_{k,j} |i, k, i + q_2, j + q_1\rangle_{a,b,q,e} \tag{26}$$

$$\Phi_2 = \frac{1}{\sqrt{d}} \sum_{i,j,k=0}^{d-1} H_{i,j} H^*_{k,j} |i, k, i + q_2, j + q_1 - i - q_2\rangle_{a,b,q,e} \tag{27}$$

$$\tag{28}$$

Note that if Eve now measures her qudit, she will not obtain $q_1 - q_2$ anymore but a variety of qudits with probabilities that we will show to be equal. In this way Alice and Bob prevent Eve from getting any information about the value of $q_1 - q_2$ by her entanglement process. To analyze the security of this protocol against this type of attack, we have to calculate a number of conditional probabilities. The notations have the standard meanings, i.e: $P_{Eve}(q|q_1, q_2)$ denotes the probability of Eve measuring her qudit to be q, provided that the first and the second qudits sent, have been q_1 and q_2 respectively. Simple calculations show that

$$P_{Eve}(q|q_1, q_2) = \langle \Phi_2 | (I \otimes I \otimes I \otimes |q\rangle\langle q|) | \Phi_2 \rangle = \frac{1}{d} \sum_{j=0}^{d-1} |H_{j,q+q_2-q_1+j}|^2 = \frac{1}{d} \tag{29}$$

where we have used the unitarity of H. This then means that Eve's probability distribution for measurement of the second qudit is completely flat (her density matrix is $\rho_{Eve} = \frac{1}{d} I$) and she gains no information by intercepting the key in this type of attack. When Eve measures her qudit to be q, the normalized state after her measurement will be:

$$\Phi_3(\text{after Eve measurement}) = \sum_{i,k=0}^{d-1} H_{i,i+q_2-q_1+q} H^*_{k,i+q_2-q_1+q} |i, k, i + q_2, q\rangle \tag{30}$$

whereupon the final state on which bob makes his measurement will be:

$$\Phi_4 = \sum_{i,k=0}^{d-1} H_{i,i+q_2-q_1+q} H^*_{k,i+q_2-q_1+q} |i, k, i + q_2 - k, i + q + q_2\rangle \tag{31}$$

Thus the conditional probability of Bob measuring the state of the received qudit to be b, provided that the first and the second qudits have been q_1 and q_2 and Eve has measured her qudit to be q, will be:

$$P_{Bob}(b|q, q_1, q_2) = \langle \Phi_4 | (I \otimes I \otimes |b\rangle\langle b| \otimes I) | \Phi_4 \rangle = \sum_i |H_{i,i+q_2-q_1+q}|^2 |H_{i+q_2-b,i+q_2-q_1+q}|^2 = \frac{1}{d} \tag{32}$$

One can now determine the probability of Bob measuring the second qudit to be b, provided that the qudit q_2 has been sent. Assuming that Alice sends all the qudits with equal probability ($P_{\text{Alice}}(q_2) = \frac{1}{d}$) We have:

$$\begin{aligned} P_{Bob}(b|q_2) &= \frac{P_{Bob}(b, q_2)}{P_{Alice}(q_2)} = d P_{Bob}(b, q_2) \\ &= d \sum_{q_1,q} P_{Bob}(b, q, q_2, q_1) = d \sum_{q_1,q} P_{Bob}(b|q, q_2, q_1) P_{Eve}(q, q_2, q_1) \end{aligned}$$

$$= \quad d \sum_{q_1,q} P_{Bob}(b|q,q_2,q_1) P_{Eve}(q|q_2,q_1) P_{Alice}(q_2,q_1) \tag{33}$$

Assuming that the consecutive qubits sent by Alice are not correlated, we have $P_{Alice}(q_2,q_1) = \frac{1}{d^2}$, and inserting the values of various probabilities from the previous equations we obtain:

$$P_{Bob}(b|q_2) = \frac{1}{d} \qquad \text{or} \qquad P_{Bob}(Error) = \frac{d-1}{d} \tag{34}$$

This then means that Eve's intercepting causes a high rate of error in the transmission of the key, specially if we use high dimensional or even continuous states. Therefore by comparing only a small fraction of their key, Alice and Bob can ascertain the presence of a third party intercepting their communication. In case they detect no intercepting, they should only discard a tiny portion of their key. In case Alice and Bob act by the local operator $U \otimes U^*$ for any unitary operator, on their initial Bell state, they can still run this protocol with success, and a repetition of the above calculations on conditional probabilities show that the probability of error for Bob will be $1 - \frac{1}{d}\sum_{i,j=0}^{d-1} |U_{i,j}|^4$. Choosing the Hadamard gate for U, is in a sense the optimum choice, in that it maximizes the above probability.

4 Discussions

There has been a lot of interest toward quantum computation and quantum communication with continuous variables in the past couple of years (see [10, 11] and references therein), where instead of bits, information may be stored in infinite dimensional states like position or momentum of a particle or amplitude of an electromagnetic field. Part of this interest derives from the fact that it has been shown that a combination of optical devices like phase shifters and beam splitters may be sufficient to act as a set of universal gates. Therefore many algorithms and protocols have been re-studied for continuous variables [11]. Now that we have a QKD protocol for d-level states for any d, a natural question arises whether it is possible to go to a proper continuous limit and define the above process for continuous variables. Naively one can generalize the definition of Bell states as follows:

$$|\Psi_{\alpha,\beta}\rangle = \frac{1}{\sqrt{2\pi}} \int e^{i\beta x} |x, x+\alpha\rangle \tag{35}$$

where α and β are continuous labels ranging from $-\infty$ to $+\infty$ and $|x\rangle$ is a continuous state like position and all the integrals now and hereafter are over the real line. These states are normalized in the sense that

$$\langle \Psi_{\alpha,\beta} | \Psi_{\alpha',\beta'} \rangle = \delta(\alpha - \alpha')\delta(\beta - \beta') \tag{36}$$

and are maximally entangled in the sense that $trace_2(|\Psi_{\alpha,\beta}\rangle\langle\Psi_{\alpha,\beta}|) \propto I$. The generalization of the Hadamard operator is nothing but the Fourier transform operator which

has already been used in [11] to generalize the Grover algorithm [17] to continuous domain.

$$H|x\rangle = \frac{1}{\sqrt{2\pi}} \int e^{ixy}|y\rangle \tag{37}$$

The controlled right shift operator now takes the form

$$R_c|x, y\rangle = |x, x + y\rangle \tag{38}$$

which as an operator takes the particularly simple form

$$R_c = e^{-iX\otimes P} \tag{39}$$

However using these continuously labeled states in the protocol one runs into difficulty in computing various probabilities, due to their ill-defined normalization. One possible solution may be to first define a infinitely countable set of bell states for two particles in a box. This however is not an easy task.

5 References

1. M. A. Nielson and I. L. Chuang; Quantum Computation and Information , *Cambridge, University Press*, 2000).

2. J. Preskill; Quantum Computation, lecture notes.

3. A. Steane, Rep. Prog. Phys. **61**, 117 (1198).

4. S. D. Bartlett, H. de Guise, and B. C. Sanders; Quantum Computation with Qudits in spin systems and harmonic oscillators, quant-ph/0109066.

5. E. Knill; Non-binary unitary error bases and quantum codes, quant-ph/9608048.

6. H. F. Chau; Correcting quantum errors in higher spin systems, quant-ph/9610023.

7. C. H. Bennet and G. Brassard, in *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Banglore, India*, 1984 (IEEE, New York, 1984), p. 175.

8. N. Cerf, M. Bourennane, A. Karlsson and N. Gisin; Security of quantum key distribution using d-level systems, quant-ph/0107130.

9. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden; Quantum Cryptography, quant-ph/0101098.

10. S. L. Braunstein, Phys. Rev. Lett., **80**, 4084, (1998).

11. A. K. Pati, S. L. Braunstein, and S. Loyd; Quantum Searching with Continuous variables, quant-ph/0002082.

12. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A, **61** 062308 (2000).

13. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

14. A. Cabello, Quantum key distribution without alternative measurements, quant-ph/9911025.

15. Y. S. Zhang, C. F. Li, and G. C. Guo; Phys. Rev. A, **64** 024302, (2001).

16. N. J. Cerf, Phys. Rev. Lett. **84** 4497 (2000); J. Mod. Opt. **47**, 187 (2000), Acta Phys. Slov. **48**, 115 (1998).

17. L. K. Grover, Phys. Rev. Lett. **79** 325 (1997).

18. D. Deutch, Proc. of R. Soc. London, A**400**, 97 (1985).

19. D. Deutch, and R. Josza, Proc. of R. Soc. London, A**439**, 553 (1992).

20. E. Bernstein and U. Vazirani, Proceeding of the 25th annual symposium on the theory of computing, ACM press, 11-20, 1993.

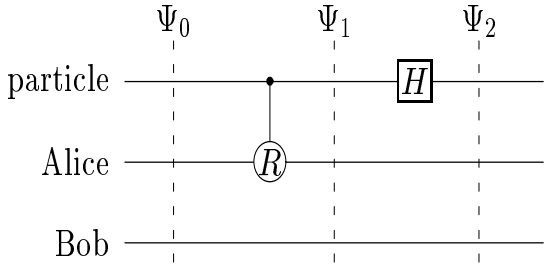

Figure 4: Teleportation using the generalized Bell states

Appendix

The problems discussed in the appendix are of minor importance and are only presented to show that almost all the simple algorithms and protocols can be generalized to the d-level case.

5.1 Teleportation Using the generalized Bell states

Using the Hadamard and controlled -shift gates one can also teleport $d-$dimensional states exactly in the same manner for $2-$ level bits. The circuit is shown in fig. (4), where the first line shows the state of the particle and the second and the third lines show respectively the states of Alice and Bob. Alice and Bob are of course assumed to be separated in space. The state of the particle to be teleported is $|\Psi_p\rangle = \sum_0^{d-1} \alpha_i |i\rangle$. The initial state of the particle (p), Alice (a), and Bob (b) is:

$$|\Psi_0\rangle_{p,a,b} = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \alpha_i |i,j,j\rangle \tag{40}$$

After the right-shift this state is transformed into:

$$|\Psi_1\rangle_{p,a,b} = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \alpha_i |i,i+j,j\rangle \tag{41}$$

and after the Hadamard gate into:

$$|\Psi_2\rangle_{p,a,b} = \frac{1}{d} \sum_{i,j,k=0}^{d-1} \alpha_i \zeta^{ik} |k,i+j,j\rangle \tag{42}$$

$$= \frac{1}{d} \sum_{k,s}^{d-1} |k,s\rangle \sum_{j=0}^{d-1} \alpha_{s-j} \zeta^{(s-j)k} |j\rangle \tag{43}$$

$$=: \frac{1}{d} \sum_{k,s}^{d-1} |k,s\rangle |\Phi(k,s)\rangle \tag{44}$$

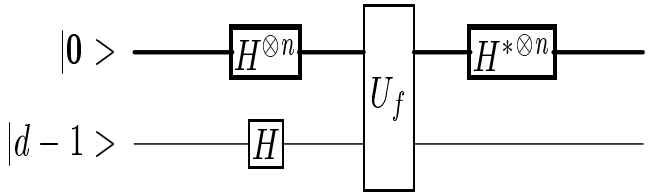

Figure 5: Generalizing quantum algorithms to qudits

which means that when Alice measures the particle and her state in the state $|k, s\rangle$, Bob's state is projected to $|\Phi_{k,s}\rangle$. At this step Alice can inform Bob the pair (k,s) and Bob can retrieve the state of the particle by acting on his state by $U_{-s,-k}$:

$$U_{-s,-k}|\Phi(k,s)\rangle = \zeta^{-sk}\sum_{j=0}^{d-1}\alpha_j|j\rangle \tag{45}$$

The inverse of this process, that is dense coding can obviously be carried out similarly with d level states.

5.2 Simple Quantum Algorithms for d-level Systems

With the simple circuit of fig. (5), we can generalize various simple algorithms with slight modifications in the proofs to the case of qudits. As a simple example we show how the generalization of Deutch [18], Deutch-Josza [19], and the Bernstein-Vazirani[20] Problems are solved for qudits.
If we restrict ourselves to linear function $f(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x} + b$ from Z_d^n to Z_d (the number of which is d^{n+1} compared to the total of d^{d^n} functions), then the coefficient of the linear term $\mathbf{a} \in Z_d^n$, can be determined with certainty, by one call of the oracle. In fact it is quite easy to see that the output state of the circuit in fig. (5) is modulo an overall phase ζ^b equal to

$$|\Psi_{out}\rangle = \frac{1}{d^{n+\frac{1}{2}}}\sum_{\mathbf{x},\mathbf{y},i}\zeta^{-i-\mathbf{x}\cdot\mathbf{y}}|\mathbf{y}, \mathbf{a}\cdot\mathbf{x}+j\rangle = \frac{1}{d^{n+\frac{1}{2}}}\sum_{\mathbf{x},\mathbf{y},j}\zeta^{-j+\mathbf{x}\cdot(\mathbf{a}-\mathbf{y})}|\mathbf{y}, j\rangle \tag{46}$$

which after simple algebra turns out to be $|\mathbf{a}\rangle|-\rangle$ where $|-\rangle := H|d-1\rangle = \frac{1}{\sqrt{d}}\sum_i \zeta^{-i}|i\rangle$. Hence measuring the first register gives the exact value of the coefficient $\mathbf{a}$. Incidentally this shows that the generalization of the Bernstein-Vazirani problem, which is to determine by one call of the oracle, the value of $\mathbf{a}$ in the function $f(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x}$, can also be solved by the same circuit.
Note that as far as functions from Z_2 to Z_2 are concerned, all functions are linear $f(x) = a_1x + a_0$, and the value of a_1 determines if they are constant ($a_1 = 0$) or balanced ($a_1 = 1$). This is the simple Deutch problem.
We can also adhere to the literal interpretation of the Deutch-Josza algorithm and this time restrict ourselves to the subset of constant or balanced functions and again

determine by one call of the oracle if the function is constant or balanced. (Note that by a balanced function we mean $|I_k| \equiv |\{x|f(x) = k\}| =$ independent of k.)
To see this we note that the state after the action of U_f in fig. (5) is

$$|\Psi_1\rangle = \frac{1}{d}\sum_{x,i}\zeta^{-i}|x, f(x)+i\rangle = \frac{1}{d}\sum_{x,j}\zeta^{f(x)-j}|x,j\rangle \quad (47)$$

$$= \frac{1}{\sqrt{d}}\sum_{x}\zeta^{f(x)}|x\rangle|-\rangle \quad (48)$$

If the function is constant then this output state, when passed through the Hadamard gate gives $|0\rangle|-\rangle$, and thus the measurement of the first register gives with certainty the value 0. However if the function is balanced it will yield all values except 0. In fact we can rewrite $\sum_x \zeta^{f(x)}|x\rangle$ as $\sum_{k=0}^{d-1}\sum_{x\in I_k}\zeta^k|x\rangle$ and use:

$$\langle 0|H^*|\sum_{k=0}^{d-1}\sum_{x\in I_k}\zeta^k|x\rangle = \sum_{k=0}^{d-1}\sum_{x\in I_k}\zeta^k\langle 0|H^*|x\rangle \quad (49)$$

$$= \sum_{k=0}^{d-1}\sum_{x\in I_k}\zeta^k\sum_{y}\delta_{y,x} = \sum_{k=0}^{d-1}\sum_{x\in I_k}\zeta^k \quad (50)$$

$$= |I_0|(\sum_{k=0}^{d-1}\zeta^k) = 0 \quad (51)$$

The Simon problem can be stated and solved for qudits quite similarly to the above. Therefore as far as quantum algorithms and quantum circuits are concerned, there is a uniform method of treating qudits for any d, including $d = 2$. One needs to replace the CNOT and the Hadamard gates appropriately.